Forschungsschwerpunkte – Dr. Thorsten Holz

Mein wissenschaftlicher Anspruch und mein persönliches Interesse werden vereint durch das Gebiet der Systemsicherheit (Systems Security) mit all seinen Facetten wie Analyse, Modellierung, Entwurf, Implementierung und Validierung von Systemen. Ich beschäftige mich mit verschiedenen Themen aus dem Gebiet der systemnahen IT-Sicherheitsforschung. Dieses System zeichnet sich dadurch aus, dass dort immer die Sicherheit konkreter Systeme und die Sicherheitsauswirkungen realer Phänomene im Mittelpunkt des Interesses stehen. Am Ziel meiner Forschungsanstrengungen steht eine praktisch verwertbare Entwurfsmethodik für die Entwicklung sicherer Systeme und die prototypische Umsetzung dieser Ansätze. Insbesondere mit den Bereichen zuverlässige vernetzte Systeme und Sicherheit von Betriebssystemen habe ich mich in den vergangenen Jahren intensiv beschäftigt. Dabei standen vor allem die verhaltensbasierte Analyse von Schadsoftware, Schutzmaßnahmen gegen Angriffe und die Untersuchung moderner Bedrohungen im Vordergrund meiner Forschung.

Aktuell beschäftige ich mich vor allem mit der Analyse von Schadsoftware: Angriffe im Internet sind heute zumeist verursacht durch bösartige Software (engl. malicious software, kurz: Malware), die sich autonom verbreitet und dabei in großem Maßstab verwundbare Rechner im Internet infiziert. Beispiele für derartige Malware sind Würmer, Trojanische Pferde, Viren und Bots. Insbesondere der Zusammenschluss von Bots zu großen Botnetzen stellt eine ernst zu nehmende Gefahr für das Internet dar. Im Folgenden wird ein kurzer Überblick zu den grundlegenden Themengebieten Honeypots/Honeynets und Botnetze, die im Rahmen meiner Arbeit behandelt wurden, gegeben. In beiden Bereichen wurden technische Grundlagen erarbeitet, neuartige Tools und Techniken entwickelt sowie empirische Untersuchungen im Internet durchgeführt.

Honeypots und Honeynets: Der englische Begriff Honeypot bezeichnet für gewöhnlich einen Gegenstand, von dem eine gewisse Attraktivität ausgeht, die bestimmte, nicht nur tierische Interessenten anzulocken vermag. Ein Honeypot eignet sich demnach als Köder, um Aufmerksamkeit auf einen bestimmten Gegenstand zu lenken. Dieses Prinzip der Köderung kann auch im Bereich der IT-Sicherheit angewendet werden: Hier werden elektronische Köder ausgelegt, um das Verhalten von Angreifern leichter zu studieren. Elektronische Köder sind Netzwerkressourcen (zum Beispiel Computer, Router oder Switches), deren Wert darin besteht, angegriffen und kompromittiert zu werden. Diese Honeypots haben keine spezielle Aufgabe im Netzwerk, sind aber ansonsten nicht von regulären Komponenten zu unterscheiden und dienen als Lockmittel für Angreifer. Sie sind mit spezieller Soft-

ware ausgestattet, welche die anschließende Forensik eines Angriffs deutlich erleichtert. Im Gegensatz zu einer herkömmlichen forensischen Untersuchung erlauben beispielsweise gezielte Veränderungen im Betriebssystem das direkte Mitschneiden aller Aktivitäten eines Angreifers. Durch die Vielfalt der gewonnenen Daten kann man schneller und genauer dessen Angriffswege, Motive und Methoden erforschen.

Botnetze: Ein Botnetz ist ein Netz aus kompromittierten Maschinen, die unter der Kontrolle eines Angreifers stehen. Der Angreifer kann Befehle zu den einzelnen Bots senden und diese führen diese Kommandos aus. Der Angreifer kommuniziert über den sogenannten Command-and-Control-Server mit den kompromittierten Maschinen: Die Bots verbinden sich zu dem C&C-Server, über den sie die Kommandos empfangen, und durch diesen Mechanismus hat ein Angreifer eine vollständige Kontrolle über diese Maschinen. Botnetze werden von Angreifern häufig zum Versenden von Spam-Nachrichten, zur Durchführung von Distributed-Denial-of-Service-(DDoS)-Angriffen oder zum Stehlen von Information von den kompromittierten Maschinen benutzt. Somit sind Botnetze eine der Wurzeln von Online-Kriminalität und bieten eine Plattform für diese Art von Verbrechen.

Im Rahmen der Arbeit wurden Botnetze systematisch studiert und es wurden effektive Erkennungsmethoden entwickelt, beispielsweise zur Erkennung von infizierten Maschinen. Neben Botnetzen mit einem zentralen C&C-Server existieren Botnetze, die ein Peer-to-Peer-Protokoll als Kommunikationsmechanismus implementieren: Die einzelnen Bots werden als Teil der Kommunikationsinfrastruktur benutzt und deshalb ist es deutlich schwieriger, diese Art von Botnetzen zu studieren und dagegen vorzugehen. Im Rahmen der Forschung wurden zusammen mit Kollegen verschiedene Arten von Peer-to-Peer-Botnetzen studiert, empirische Messungen durchgeführt und Gegenmaßnahmen entwickelt.

Weitere Forschungsschwerpunkte: Im Rahmen der Arbeit beschäftige ich mich mit weiteren Themen aus dem Bereich der systemnahen IT-Sicherheitsforschung, beispielsweise mit den Bereichen Sicherheit von Smartphones, Analyse von Schadsoftware, Spam und Sicherheit in sozialen Netzen. Insbesondere soziale Netze sind ein interessanter Forschungsbereich: Diese Art von Webseiten gehört zu den populärsten Seiten im Internet und Anbieter wie beispielsweise Facebook, Xing, StudiVZ oder LinkedIn haben viele Millionen Nutzer, wodurch diese für Angreifer ein lohnenswertes Ziel werden. Im Rahmen der Forschungsaktivitäten der Arbeitsgruppe wurden Sicherheitsaspekte verschiedener sozialer Netze untersucht, insbesondere das Thema Privatsphäre und mögliche Angriffe darauf wurden studiert. Wir konnten beispielsweise zeigen, wie ein Angreifer automatisiert Netzbenutzer aufgrund ihrer Mitgliedschaft in sozialen Netzen deanonymisieren kann.